It’s time for governments to help their citizens deal with cybersecurity

August 26, 2018 10.25am BST

Cybersecurity is everyone’s problem, all over the world. NicoElNino/Shutterstock

Cyber criminals are extremely active across the globe – and, unfortunately, also very successful. In Africa, too, businesses are losing billions to cybercrime.

A quick Internet search shows that governments in the Southern African Development Community aren’t really prioritising cybersecurity.

Author

Karen Renaud
Professor of Cybersecurity, Abertay University

Disclosure statement

Karen Renaud does not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and has disclosed no relevant affiliations beyond their academic appointment.

Partners

The Conversation UK receives funding from Hefce, Hefcw, SAGE, SFC, RCUK, The Nuffield Foundation, The Ogden Trust, The Royal Society, The Wellcome Trust, Esmée Fairbairn Foundation and The Alliance for Useful Evidence, as well as sixty five university members.

View the full list

Originally published in The Conversation
https://theconversation.com/its-time-for-governments-to-help-their-citizens-deal-with-cybersecurity-100771

Botswana doesn't name cyber security as one of its national priorities. Nor does Mozambique. Zambia's 2018 budget doesn't mention cybersecurity; nor does Namibia's. Yet African countries are not immune to cybercrime, as recent reports from Botswana, Zimbabwe and Mozambique show.

South Africa appears to be especially vulnerable. The US Federal Bureau of Investigationranks the country sixth and seventh on its different types of cybercrime predator list. The global WannaCry malware attack of May 2017 hit South Africa harder than any other African country. It has been estimated that South African companies on average lose R36 million when they fall victim to an attack. Small businesses will often not be able to sustain such heavy losses, and could stop trading after an attack.

South Africa published a national cybersecurity policy framework in 2012. But it's not obvious what measures have been put in place to help private individuals to become more resilient to cybercrime. This is important because, as big businesses become more proficient in repelling cyber attacks, criminals are turning their attention to small businesses and individual home users.

When it comes to the individual citizen, whose responsibility is it to guard against cybercrime? Research we've conducted suggests that governments have a crucial role to play. They need to support individual citizens, as well as businesses, in a more practical and proactive way, to manage this particular society risk.

For instance, they could provide individuals with free face-to-face assistance and cybersecurity support. They could give clear guidelines and provide government sanctioned security software for people to install, and make sure it's easy to get hold of. New York has recently started providing this kind of support to its residents. Based on our research, we believe there's scope for all governments, including those in Southern Africa, to do the same.

Managing risk

Governments have different approaches to helping their citizens manage risk. For some kinds, such as smoking in private, they issue advice and leave citizens to manage the risk themselves. These can be referred to as "solo risks".

In other cases, governments create supportive systems so that the management of a particular risk is shared between citizen and state. The split is determined by the nature of the risk and the stance adopted by the government in power. These kinds of risks can be referred to as "society risks". Road safety is a good example of this: people have to pass tests to be permitted to drive, the authorities fine and prosecute those who drive badly, and drivers pay a yearly licence to fund the road infrastructure.

A solo risk can generally be mitigated by disseminating advice to citizens. This approach is justified if only the person who does not follow the advice is harmed. However, when a failure to manage a risk harms the community at large, advice, on its own, might be insufficient.

It's fair to say that the cybersecurity risk is currently managed by governments in the same way as they treat private smoking - as if it were a solo risk. By and large, governments provide advice about cybersecurity risks and then leave citizens either to take security precautions, or not. This seems to be based on the assumption that only the individual computer or device owner suffers loss or harm if they fall victim to an attack.

In reality, cybersecurity attacks are like fire and disease. They seldom affect only one individual. Data that's stolen from one person's device is likely to include the personal details of many other people, potentially endangering the wider community. Malware and viruses also spread from one person's device to another, much like contagious diseases.

Moreover, this is not just about financial loss; it impacts privacy too. Privacy, once lost, can *never* be regained. South Africa has experienced two serious privacy violations recently, because the data had seemingly not been secured properly. Those who steal leaked personal identification data can steal identities, a harrowing experience that is very difficult to recover from.

We can conclude that the cyber risk is manifestly *not* a solo risk, but rather a society risk. Leaving citizens alone and unaided to deal with cybersecurity threats is clearly not the best long-term strategy.

Helping home users

Every country needs to formulate a behavioural intervention programme. This means that interventions are formulated according to scientifically-proven behavioural principles to maximise uptake. This would provide support so that everyone – whether they're business owners or home users – is able to repel and resist attacks. New York has made a good start, and other governments will hopefully follow suit.

Governments could work with mobile phone providers so that security-related software updates can be batched and issued via their trusted channels. They could prompt people to install these by disseminating the need for the updates using carefully crafted text messages, and also publicise this via other media outlets.

Community leaders can also be taught about cybersecurity risks and mitigations so they can become evangelists and spread the word widely throughout rural and urban centres.

Cybercrime is not going to evaporate. It's crucial for governments to help their citizens manage this social risk. This will protect incomes, reputations, personal and sensitive information and generally improve resilience across the board.

Key words: Cybersecurity, Responsibility, Cybercrime, South Africa, Zimbabwe, Malawi, Botswana, Zambia, Southern Africa, Namibia, Mozambique, Cyber attack